

Inhaltsverzeichnis

Vorwort	11
Teil 1 – Kryptographie	15
1 Angriffe auf die IT-Sicherheit und bestehende Sicherheitssysteme	17
1.1 Übersicht über bestehende TCP/IP-Sicherheitssysteme	17
1.2 Übersicht über die verschiedenen Angriffe auf die IT-Sicherheit	20
2 Grundziele der Kryptographie	25
2.1 Kryptographische Verschlüsselung	28
2.1.1 Symmetrische Verschlüsselungsverfahren	31
2.1.2 Asymmetrische, öffentliche Verschlüsselungsverfahren	34
2.2 Kryptographische Hashfunktionen	41
2.3 Message Authentication Codes	42
2.4 Digitale Signaturen	44
3 Speicherung von Zertifikaten und kryptographischen Schlüsseln	49
3.1 ASN.1, DER und BER	49
3.2 PEM-Format	53
3.3 PKCS #8 Private-Key Information Syntax	54
3.4 PKCS #12 Personal Information Exchange Syntax	56
4 X.509-Zertifikate	59
4.1 Format eines X.509-Zertifikats	60
4.1.1 X.509v3 Extensions	63
4.1.2 Beispiele für X.509v3-Zertifikate	67
4.1.3 Zertifikatsklassen (Certificate Policies)	72
4.2 CRL – Certificate Revocation List	73
4.2.1 X.509v2 CRL Format	74
4.2.2 X.509v2 CRL Extensions	76
4.2.3 Beispiel für eine X.509v2 CRL	78
5 Public Key Infrastructure (PKI)	81
5.1 Dezentrale PKI	81
5.2 Zentralisierte (hierarchische) PKI	82

5.3	PKCS – Public-Key Cryptography Standards	86
5.3.1	PKCS #6 Extended Certificate	86
5.3.2	PKCS #7 Cryptographic Message Syntax	87
5.3.3	PKCS #10 Certificate Request Syntax	94
5.4	PKIX – Internet Public Key Infrastructure X.509	99
5.5	SCEP – Simple Certificate Enrollment Protocol	103
Teil 2 – IPSec-Architektur		115
6	SA – Security Association	119
6.1	Transport und Tunnel Mode Security Association	119
6.2	Security Associations Bundle	120
6.3	Security Policy und Security Association Database	121
7	IPSec-Sicherheitsprotokolle	127
7.1	AH – Authentication Header	127
7.2	ESP – Encapsulating Security Payload	135
8	ISAKMP – Internet Security Association and Key Management Protocol	149
8.1	ISAKMP Phase I und II	150
8.2	ISAKMP Payloads	152
8.2.1	Security Association Payload	156
8.2.2	Proposal Payload	158
8.2.3	Transform Payload	159
8.2.4	Identification Payload	167
8.2.5	Key Exchange, Certificate und Certificate Request Payload	169
8.2.6	Hash, Signature und Nonce Payload	171
8.2.7	Notification Payload	172
8.2.8	Delete und Vendor ID Payload	174
8.3	ISAKMP Exchange	175
8.3.1	Aufbau einer ISAKMP Security Association	175
8.3.2	Informational Exchange	182
8.3.3	Base Exchange	182
8.3.4	Identity Protection Exchange	183
8.3.5	Authentication Only Exchange	184
8.3.6	Aggressive Exchange	185
9	IKE – Internet Key Exchange	187
9.1	New Group Mode Exchange	187
9.2	Informational Mode Exchange	188
9.3	Main und Aggressive Mode Exchange	190
9.3.1	Authentifiziertes Verschlüsselungsmaterial für ISAKMP SAs	190
9.3.2	Authentifizierung über Pre-shared Keys	194
9.3.3	Authentifizierung über Signaturen	200
9.3.4	Authentifizierung über öffentliche Verschlüsselungsverfahren	204

9.3.5	Authentifizierung über öffentliche Verschlüsselungsverfahren (Revised Mode)	206
9.4	Quick Mode Exchange	208
9.4.1	Authentifiziertes Verschlüsselungsmaterial für IPSec SAs	209
9.4.2	Perfect Forward Secrecy	211
9.5	Transaction Exchange	215
Teil 3 – IOS SSH und IPSec Konfiguration		219
10	SSH – Secure Shell	221
10.1	SSH-Server-Konfiguration	223
10.2	SSH-Client-Konfiguration	227
11	Konfiguration der ISAKMP Security Association	231
11.1	Definition der ISAKMP Protection Suite	232
11.2	Gültigkeitsdauer der ISAKMP SA	233
11.3	Authentifizierung der ISAKMP-Partner	236
11.3.1	Authentifizierung über RSA-Signaturen	236
11.3.2	Authentifizierung über Pre-shared Keys	255
11.3.3	Authentifizierung über RSA-Verschlüsselung	263
11.4	Cisco-Erweiterungen Mode Config und XAuth	275
12	Konfiguration der IPSec Security Association	279
12.1	Definition der IPSec Protection Suite	279
12.2	»set peer«-Befehl	283
12.2.1	ISAKMP Keepalive	291
12.3	»match address«-Befehl	295
12.3.1	Probleme bei Access-Listen, die nicht gespiegelt sind	300
12.4	Sicherheitsmechanismen (Transforms) definieren	304
12.5	Gültigkeitsdauer der IPSec Security Association	306
12.6	Dynamische Crypto Map	309
12.7	Tunnel Endpoint Discovery (TED)	311
12.8	IPSec und Interface-Access-Listen	315
13	IPSec-Fehlersuche	321
13.1	Debugging von ISAKMP-Nachrichten	322
13.1.1	Debugging eines Main Mode Exchange	323
13.1.2	Debugging eines Quick Mode Exchange	325
13.1.3	Debugging des Aufbaus von ISAKMP und IPSec SAs	328
13.1.4	IP Packet Debugging	332
13.2	Probleme beim Aufbau der ISAKMP Security Association	333
13.2.1	Die Crypto Map ist keinem Interface zugeordnet	333
13.2.2	Keine übereinstimmende ISAKMP Policy	334
13.2.3	Probleme mit der ISAKMP Lifetime	336
13.2.4	Probleme bei der Authentifizierung	337
13.3	Probleme beim Aufbau der IPSec Security Association	345

13.3.1	Kein übereinstimmendes Sicherheitsprotokoll (Transform)	345
13.3.2	Probleme mit dem »set peer«-Eintrag und der ISAKMP-Identität	347
13.3.3	Probleme mit der Access-Liste der Crypto Map	349
13.4	Probleme bei existierenden IPSec SAs	353
13.4.1	IPSec SA existiert nur noch auf einem System	353
13.4.2	Die Datenpakete werden trotz vorhandener SA nicht geschützt	355
13.4.3	Die Pakete passen nicht zu der Access-Liste	356
13.4.4	IPSec und Path MTU Discovery	356
Teil 4 – Windows 2000 und IPSec		361
14	IPSec-Konfiguration unter Windows 2000	363
14.1	Computer-Zertifikate für die Authentifizierung über RSA-Signaturen anfordern	363
14.2	Window-2000-Besonderheiten	368
14.2.1	Ausschalten bzw. Ändern der IPSec-Vorgaben für L2TP	368
14.2.2	Tunnel Mode Security Association	369
14.3	IPSec Debugging unter Windows 2000	370
14.4	Beispiel für die manuelle IPSec-Konfiguration unter Windows 2000	378
14.4.1	Konfiguration des Cisco Routers	378
14.4.2	Konfiguration des Windows-2000-PC	384
15	L2TP – Layer Two Tunneling Protocol	395
15.1	L2TP-Verbindung zwischen zwei Routern ohne IPSec	399
15.2	Windows 2000 und L2TP	406
15.2.1	Konfiguration des L2TP-Tunnels auf dem Client	408
15.2.2	Cisco Router als Network Access Server (NAS)	413
15.2.3	Cisco Router als L2TP Tunnel Server (LNS)	416
15.3	Manuelle Konfiguration der IPSec-Filter für L2TP	421
15.3.1	Konfiguration des Windows 2000 Clients	422
15.3.2	Konfiguration des Cisco Routers	436
15.4	L2TP-Verbindung zwischen einem Windows-2000-Client und einem Server	448
Teil 5 – Beispielkonfigurationen		455
16	Beispielkonfigurationen	457
16.1	Aushandeln der ISAKMP Protection Suite	457
16.1.1	IOS: Mehrere »crypto isakmp policy«-Einträge	457
16.1.2	VPN Client: Mehrere Proposal-Einträge für die ISAKMP SA	460
16.2	Aushandeln der IPSec Protection Suite	463
16.2.1	IOS: Mehrere Sicherheitsprotokolle über eine IPSec-Verbindung	463
16.2.2	IOS: Auswahl zwischen mehreren Sicherheitsprotokollen	468
16.2.3	VPN Client: Auswahl zwischen mehreren Sicherheitsprotokollen	473
16.3	Manuelle Definition einer ESP Security Association	475
16.4	Authentifizierung der ISAKMP-Partner	480

16.4.1	Authentifizierung über Pre-shared Keys mit IP-Adresse als ISAKMP-Identität	480
16.4.2	Authentifizierung über Pre-shared Key mit Domainnamen als ISAKMP-Identität	489
16.4.3	Authentifizierung über RSA-Signaturen (VPN Client – Cisco Router)	491
16.5	IPSec in großen Netzwerken	510
16.5.1	»Hub and Spoke«-Topologie	510
16.5.2	»Fully-meshed«-Topologie	543
16.5.3	Schutz anderer Protokolldaten mit Hilfe eines GRE-Tunnels	558
16.5.4	IPSec und HSRP	573
16.5.5	IPSec und NAT	594
17	Ausführlicher Trace einer IPSec-Verbindung	603
17.1	Konfiguration des Cisco Secure VPN Client	603
17.2	Konfiguration des Cisco Router	607
17.3	Aggressive Mode Exchange mit Authentifizierung über Pre-shared Keys	608
17.3.1	Informationen vom VPN Client und vom Cisco Router	608
17.3.2	Trace des Aggressive Mode Exchange	612
17.3.3	Trace des Quick Mode Exchange	620
17.3.4	Verschlüsselung der Nutzdaten über die aufgebaute ESP SA	625
17.4	Main Mode Exchange mit Authentifizierung über Pre-shared Keys	627
17.4.1	Informationen vom VPN Client	627
17.4.2	Informationen vom Cisco Router	629
17.4.3	Trace des Main Mode Exchange	642
17.4.4	Quick Mode Exchange	652
17.4.5	Ablauf der IPSec Lifetime	658
17.4.6	Erneuter Ablauf der IPSec Lifetime	665
17.4.7	Ablauf der ISAKMP Lifetime	672
Anhang A: Befehlsübersicht		689
Anhang B: Beispielübersicht		693
Anhang C: Übersicht der Fehlermeldungen		695
Anhang D: Übersicht über Traces		697
Anhang E: Übersicht über Request for Comment		699
Anhang F: Abkürzungsverzeichnis		703
Anhang G: Object Identifier		707
Stichwortverzeichnis		713